Wipro’s

Encryption Policy

**Document Control**

|  |  |
| --- | --- |
| Function | Group Chief Information Security Office (GCISO) |
| Sub-function | - |
| Policy Owner | Lakshminarayanan RS, Group Head - Information Security Policy & Framework |
| Policy Effective Date | October 26, 2018 |

**Purpose**

This policy establishes the need for effective use of cryptography, encryption, and key management to protect the confidentiality, integrity, and availability of information based on business and information security requirements.

**Audience**

Organization’s employees, retainers, contractors, and service providers.

**Scope**

This policy applies to the information systems owned or managed by the Organization.

**Policy Details**

**EP.1** The Organization shall implement cryptography, encryption, and key management to comply with the requirements derived from the business, laws, regulations, and contracts.

**EP.2** Data at rest, in use, and in transit shall be encrypted as per the Cryptography and Key Management Standard.

**EP.3** The information owner shall ensure the implementation of appropriate encryption techniques to protect the information.

**EP.4** Appropriate security controls shall be implemented to protect the confidentiality and integrity of the cryptographic hashes, encryption keys, and backup.

**EP.5** The information system administrators shall comply with the Key Management process as defined in the Cryptography and Key Management Standard.

**EP.6** The digital signature owner shall be accountable for the transactions and safe maintenance of the assigned digital signature.

**EP.7** Logging and monitoring of the Key Management activities shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

| **Definition** | **Description** |
| --- | --- |
| Cryptography | The discipline embodies the principles, means, and methods for the transformation of data to hide their semantic content and prevent their unauthorized use or undetected modification. |
| Data at rest | Data stored safely on an internal or external storage. |
| Data in transit | Data transferred between locations over a private network or the Internet. |
| Data in use | Data currently being updated, processed, erased, accessed, or read by a system. |
| Digital Signatures | The result of a cryptographic transformation of data that provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation. |
| Encryption | The process of changing plain text into cipher text using a cryptographic algorithm and key. |
| Information systems | A set of applications, services, information technology assets, or other information-handling components. |
| Key Management | The management of cryptographic keys throughout its lifetime, including generation, storage, establishment, input and output, as well as use and destruction of the encryption keys. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |

**References**

* Cryptography and Key Management Standard
* Logging and Monitoring Standard
* Cryptography and Key Management Guidelines

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 27th June 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Aarti Bansal Lamba | Lakshminarayanan RS | 15th January 2024 |